Contents

Contents 1

COMMON NUMBERS OF SETS i

Cartesian Product and Mapping 1

Relations 1

1 Group 4

1.1 Subgroup 5

1.2 Cosets 8

1.3 Normal Subgroup 9

1.4 Homomorphisms 9

1.5 Kernel 11

References 12

COMMON NUMBERS OF SETS

Abbreviations	Descriptions
$\mathbb{N}$	Natural numbers $\{1, 2, 3, \cdots\}$.
$\mathbb{W}$ or $\mathbb{N}_\circ$	Whole numbers $\{0, 1, 2, 3, \cdots\}$.
$\mathbb{Z}$	Integers $\{\cdot, -1, 0, 1, \cdots\}$.
$\mathbb{Q}$	Rational numbers p/q q and p are integers.
$\mathbb{I}$	Irrational numbers {Non-rational numbers}.
$\mathbb{R}$	Real numbers {All of the above number sets}.
Imaginary Numbers	{ Numbers containing $i = \sqrt{-1}$ }.
$\mathbb{C}$	Complex numbers $\{a + bi,$ a and b are Real, $i = \sqrt{-1}\}$.

Cartesian Product and Mapping

Given Sets A and B we can define a new set $A \times B$, called the `Cartesian Products` of A and B as a set of ordered pairs that is

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\} \tag{1}$$

.

Example 1 [3] If

$$A = \{x, y\}, \;\; B = \{1, 2, 3\} \text{ and } c = \phi$$

then $A \times B$ is the set
$A \times B = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$
$A \times C = \phi$.

Relations

Definition 1 [8] A binary Relation or simply a relation R from a set A into a set B is a subset of $A \times B$.
Let R be a relation from a set A into a set B.

- If $(x, y) \in R$ we write xRy or $R(x) = y$.
- If xRy then sometimes we say that x is relation to y (or y is a relation with x) with respect to R or simply x is related to y.
- If $A = B$ then we speak of a binary relation on A.

Example 2 [8] Consider the set of integers $\mathbb{Z}$.
Let R be the set of all ordered pairs (m, n) of integers such that $m < n$, i.e

$$R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z},\ m < n\}$$

then R is a binary relation on $\mathbb{Z}$.

Definition 2 [8] Let R be a relation from a set A into a set B, then the **Domain** of R denoted by $D(R)$ is defined to be the set

$$\{x : x \in A \text{ and there exists } y \in B \text{ Such that } (x, y) \in R\} \tag{2}$$

The **Range** or **image** of R denoted by $I(R)$ is defined to be the set

$$\{y : y \in B \text{ and there exists } x \in A \text{ Such that } (x, y) \in R\} \tag{3}$$

Example 3 [8] Let $A = \{4, 5, 7, 8, 9\}$ and $B = \{16, 18, 20, 22\}$. Define by $R \subseteq A \times B$ by $R = \{(4, 16), (4, 20), (5, 20), (8, 18), (9, 18)\}$ then R is a relation from A into B, here $(a, b) \in R$ if and only if a divides b, where $a \in A$ and $b \in B$. Note that for the domain of R, we have $D(R) = (4, 5, 8, 9)$ and for the range of R we have $I(R) = \{16, 18, 20\}$.

Definition 3 [8] Let R be a binary operation on a set A then R is called

1. reflexive, if for all $x \in A$, xRx.
2. symmetric, if for all $x, y \in A$, xRy implies yRx.
3. transitive, if for all $x, y, z \in A$, xRy and yRz imply xRy.

Definition 4 [8] A binary relation E on a set A is called an **Equivalence relation** on A is E is reflexive, symmetric and transitive.

Example 4 [8] Relation

$R_1 = \{(1, a), (2, a)\} \qquad \Rightarrow 1Ra = (1, a)$

$R_2 = \{(3, b)\} \qquad\qquad 2Ra = (2, a)$.

Example 5 [8] Reflexive

Let $A = \{1, 2, 3\}$

$R_1 = \{(1, 1), (2, 2), (3, 3), (2, 3)\}$

$R_2 = \{(1, 2), (2, 2)\}$

R is Reflexive.

Example 6 [8] Symmetric

Let $A = \{a, b, c, d\}$ and R be a relation on A denoted by $R = \{(a, a), (c, c), (a, d), (d, a)\}$

Then R is symmetric.

Example 7 [8] Transitive

Let $A = \{a, b, c, d\}$ and

$R_1 = \{(a, b), (b, a), (a, a)\}$

R_1 is not transitive because $bRa \wedge aRb$

$R_2 = \{(b, c)\}$

R_2 is transitive.

Example 8 [8] Let $A = \{1, 2, 3, 4, 5, 6\}$ and

$E = \{(1, 1), (2, 2), (3, 3)(4, 4), (5, 5), (6, 6), (2, 3), (3, 2)\}$, then E is an equivalence relation on A.

Chapter 1

Group

Definition 1.1 [8] A group is an ordered pair $(G, \star)$, where G is a nonempty set and $\star$ is a binary operation on G such that the following properties hold:

G_1 : For all $a, b, c \in G$

$a \star (b \star c) = (a \star b) \star c$ (Associative law).

G_2 : There exists $e \in G$ such that for all $a \in G$,

$a \star e = a = e \star a$ (Existence of an Identity).

G_3 : For all $a \in G$ there exists $b \in G$ such that

$a \star b = e = b \star a$ (Existence of Inverse).

Thus, a group is **Mathematical system** $(G, \star)$ satisfying axioms G_1 to G_3.

Example 1.1 [8] Consider $\mathbb{Z}$ the set of integers together with the binary operation $+$, where $+$ is the usual addition we know that $+$ is associative. Now $0 \in \mathbb{Z}$ and for all $a \in \mathbb{Z}$,
$a + 0 = a = 0 + a$.
So 0 is an Identity. Also for all $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ and
$a + (-a) = 0 = (-a) + a$.
That is, $-a$ is an inverse of a. It now follows that $(\mathbb{Z}, +)$ satisfies axioms G_1 to G_3. So $(\mathbb{Z}, +)$ is a group.

Definition 1.2 [8] A **Semi group** is an ordered pair $(S, \star)$, where S is a non-empty set and $\star$ is an associative binary operation on S.
Thus, a semi group is a mathematical system with one binary operation such that the binary operation is associative.

Remark 1.1 [8] Every group is semi group but the converse is not true in general.

Example 1.2 [8] Let S be a set has more than one element we define an operation ($\star$) as follows:

$$a \star b, \ \forall \ a, b \in S$$

Show that $(S, \star)$ is a semi group but it is not group. Now, since for all a, b and $c \in S$

$i:\ a \star b = b \in S.$

$ii:\ a \star (b \star c) = (a \star b) \star c$

$a \star (b \star c) = (a \star b) \star c$

$a \star (b \star c) = a \star c = c$

$(a \star b) \star c = b \star c = c$ Then $\star$ is associative.

Thus, $(S, \star)$ is a semi group
Now, we show that $(S, \star)$ is not group
Since S has more than one element then cheese on element $x \in S$ such that $x \neq e$.
Then we get $x \star e = e$ and $e \star x = x$ $i.e$ by definition of identity $x = e$ which is a contradiction and thus S has no identity.
Hence $(S, \star)$ can not group.

1.1 Subgroup

A subset H of a group G is said to be a subgroup if, with the same operation and Identity element as that used in G it is a group.

Remark 1.1.1 [8] For each group $(G, \star)$ there exist at least two subgroup $(e, \star)$ and $(G, \star)$ this two subgroups are often namely **trivial subgroups**. Any subgroup deferent from this subgroup deferent from this subgroups is called **proper subgroup**.

Theorem 1.1.1 Let $(G, \star)$ be a subgroup and $H \neq \phi \subseteq G$, then $(H, \star)$ is a subgroup of G iff:

1. For all $a, b \in H \Rightarrow a \star b \in H$.
2. For all $a \in H \Rightarrow \exists\ a^{-1} \in H$.

Proof:

$\Rightarrow$ It is clear since $(H, \star)$ is group hence 1 and 2 are true.

$\Leftarrow$ To show that $(H, \star)$ is subgroup $i.e$ $(H, \star)$ is a group $\because$ $H \neq \phi$ and $H \subseteq G$

2 : $a \star b \in H \ \forall \ a, b \in H$ by (1)

$\star$ is binary operation on H.

3 : $\forall \ a, b$ and $c \in H$, $H \subseteq G$ then a, b and $c \in G$. So $(a \star b) \star c = a \star (b \star c)$ since G is group then $\star$ is associative of H.

4 : $\forall \ a \in H$, $\exists \ a^{-1} \in H$ then $a \& a^{-1} \in G$. SO $a \star a^{-1} = e \in H$ then $\exists \ e \in H$, $\forall \ a \in H$

$a \star e = e \star a = a$

$\star$ is Identity.

5 : For all $a \in H$, $\exists \ a^{-1} \in H$ by (1)

then $a \star a^{-1} \in H$

then $a \star a^{-1} \in G$

Hence $a \star a^{-1} = a^{-1} \star a = e$

Thus, $(H, \star)$ is a group

But $H \neq \phi \subseteq G$

Then $(H, \star)$ is a subgroup of $(G, \star)$.

Theorem 1.1.2 [8] Let $(G, \star)$ be a subgroup and $H(\neq \phi) \subseteq G$ then $(H, \star)$ is a subgroup of $(G, \star)$ iff $a \star b^{-1} \in H \ \ \forall \ a, b \in H$.

Proof:

$\Rightarrow$ Let $(H, \star)$ be a subgroup T.P $a \star b^{-1} \in H$, $\forall \ a, b \in H$

It is clear since H is subgroup then H is a group, hence, $\forall \ a, b \in H \ \Rightarrow b^{-1} \in H$ then $a \star b^{-1} \in H$.

$\Leftarrow$ Let $a \star b^{-1} \in H$, $\forall \ a, b \in H$ T.P $(H, \star)$ be a subgroup $i.e$ To show $(H, \star)$ is group

1. $H \neq \phi$, $H \subseteq G$.
2. $\star$ associative on H.

   Let a, b and $c \in H$ To prove $a \star (b \star c) = (a \star b) \star c$

   Since $H \subseteq G$ Then a, b and $c \in G$ and G is a group then

   $a \star (b \star c) = (a \star b) \star c$.

3. Since ($H \neq \phi$), then there exist $b \in H$ then by the given assumption we get $b \star b^{-1} \in H$.

   $\Rightarrow\ b \star b^{-1} \in G$ since $H \subseteq G$

   $\Rightarrow\ b \star b^{-1} = e \in H$

   Now $a \in H$ then $a \in G$ we get

   $a \star e = e \star a = a\ \ \forall\ a \in H$

   then e is the identity of H.

4. Inverse

   $\forall\ a \in H \rightarrow$ then $\forall\ a^{-1} \in H,\ \forall\ a^{-1},\ e \in H$

   $\rightarrow a^{-1},\ e \in H$

   $a^{-1} \star e \in H$

   $a^{-1} \in H$.

5. Closer

   $\forall\ a, b \in H$ T.P $a \star b \in H$

   $\forall\ a, b \in H \Rightarrow a, b^{-1} \in H$ Since $\forall$ element has clouse then $a \star (b^{-1})^{-1} \in H \Rightarrow a \star b \in H$

   then $\star$ is clouser, $\star$ is binary operation

   then $(H, \star)$ is group and $H \subseteq G$

   Hence, $(H, \star)$ is a subgroup of $(G, \star)$.

Theorem 1.1.3 [8] Let H and K are two subgroups of group $(G, \star)$, then $H \cap K$ is a subgroup of group $(G, \star)$.

Proof:

$H \cap K = \phi$ (since $e \in H \cap K$)

$H \cap K \subseteq G$

Let $a, b \in H \cap K$ to prove $a \star b^{-1} \in H \cap K$

$\Rightarrow\ a, b \in H$ and $a, b \in K$

$\Rightarrow\ a \star b^{-1} \in H$ and $a \star b^{-1} \in K$

(Since H and K are group)

Then $a \star b^{-1} \in H \cap K$

Hence, $H \cap K$ is a subgroup of G.

Theorem 1.1.4 [8] Let H and K be a subgroup of a group G, then HK is a subgroup of G

if and only if $HK = H \cup K$.

Proof:

First suppose that HK is a subgroup of G, we show that $HK = H \cup K$.

Let $h \in H$ then $h = he \in HK$,

Thus $H \subseteq HK$. Similarly, $K \subseteq HK$.

Hence $H \cup K = HK$. Now $H \cup K$

is the smallest subgroup of G containing $H \cup K$, so it follows that $H \cup K \subseteq HK$.

Let $hk \in HK$, where $h \in H$ and $k \in K$

Because $H \subseteq (H \cup K)$ and $K \subseteq (H \cup K)$

we have $h, k \in (H \cup K)$

Thus $hk \in (H \cup K)$ this implies that

$HK \subseteq (H \cup K)$. Hence $HK = H \cup K$

The converse is immediate because $(H \cup K)$ is a subgroup and $HK = (H \cup K)$.

1.2 Cosets

Definition 1.2.1 *[8] Let G be a group and H be a subgroup of G, for each element a of G we define $a \star H = \{a \star h \mid \ h \in H\}$ we call $a \star H$ the Coset of H in G generated by a.*

Remark 1.2.1 [8] In the case of additive notation the coset of H in G generated by a is written i the form

$$a + H = \{a + h \mid h \in H\}$$

Sometimes $a \star H$ is called left coset and the set $H \star a = \{ha \mid h \in H\}$ is called right coset, since we will only use left cosets, we will leave if the modifier left.

Example 1.2.1 [8] Let $\mathbb{R}$ be a set of real numbers and $\mathbb{Z}$ be the set of integers.

$(\mathbb{R}, +)$ is a group and $\mathbb{Z} \subseteq \mathbb{R}, \ \mathbb{Z} \neq \phi$.

$(\mathbb{R}, +)$ is a group, then $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{R}, +)$ denoted $\mathbb{Z} \subseteq \mathbb{R}$.

1.3 Normal Subgroup

The subgroup H is said to be normal in G if

$$g \star H = H \star G \text{ For all } g \in H$$

We write $H \lhd G$ or $H \unlhd G$ to include that H is normal subgroup of G.

Example 1.3.1 [3] Let G be an abelian group. Every subgroup H of G is a normal subgroup. Since $g \star h = h \star g$ for all $g \in G$ and $h \in H$, it will always be the case that $gH = Hg$.

Theorem 1.3.1 [3] Let G be a group and N be a subgroup of G the the following statements are equivalent

1. The subgroup N is normal in G.
2. For all $g \in G,\ gNg^{-1} \subset N$.
3. For all $g \in G,\ gNg^{-1} = N$.

Proof:

$1 \rightarrow 2$ Since N is normal in G, $gN = Ng\ \forall g \in G$. Hence for a given $g \in G$ and $n \in N$, $\exists\ n^{-1} \in N$ such that $gn = n'g$ therefore, $gng^{-1} = n' \in N$ or $gNg^{-1} \subset N$.

$2 \rightarrow 3$ Let $g \in G$. Since $gNg^{-1} \subset N$, we need only show $n \subset gNg^{-1}$. For $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Hence $g^{-1}ng = n'$ for some $n' \in N$ therefore, $n = gn'g^{-1}$ is in gNg^{-1}.

$3 \rightarrow 1$ Suppose that $gNg^{-1} = N\ \forall g \in G$ then for any $n \in N$ there exist an $n' \in N$ such that $gng^{-1} = n'$ consequently $gn = n'g$ or $gN \subset Ng$. Similarly, $Ng \subset gn$.

1.4 Homomorphisms

A homomorphism between groups $(G, \cdot)$ and $(H, \circ)$ is a map $\phi : G \rightarrow H$ such that

$$\circ\phi(g_1, g_2) = \phi(g_1) \circ \phi(g_2)$$

for all $g_1, g_2 \in G$.

Example 1.4.1 [3] Let G be a group and $g \in G$. Define a map $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a group homomorphism. Since $\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m) \cdot \phi(n)$. This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g.

Proposition 1.4.1 [3] Let $\phi : G_1 \to G_2$ be a homomorphism of group then:

1. If e is the identity of G_1, then $\phi(e)$ is the identity of G_2.
2. For any element $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$.
3. If H_1 is a subgroup of G_1, then $\phi(H_1)$ is subgroup of G_2.
4. If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ is a subgroup of G_1 furthermore, if H_2 is normal in G_2 then $\phi^{-1}(H_2)$ is normal in G.

Proof:

1. Suppose that e and e' are the identities of G_1 and G_2 respectively then

   $$e'\phi(e') = \phi(e) = \phi(ee) = \phi(e)\phi(e)$$

   by cancellation $\phi(e) = e'$.

2. This statement follows from the fact that $\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi e = e'$.

3. The set $\phi(H_1)$ is nonempty since the identity of G_2 is in $\phi(H_1)$ suppose that H_1 is a subgroup of G_1 and let x and y be in $\phi(H_1)$ there exist an elements $a, b \in H$, such that $\phi(a) = x$ and $\phi(b) = y$ since
   $xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(ab^{-1}) \in \phi(H_1)$ is subgroup.

4. Let H_2 be a subgroup of G_2 and define H_1 to be $\phi^{-1} \in H_2$, that is H_1 is the set of $g \in G_1$ such that $\phi(y) \in H_2$. The identity is in H_1 since $\phi e = e'$. If a and b are H_1, then $\phi(ab^{-1}) = \phi(a)[\phi(b)]^{-1}$ is in H_2, since H_2 is subgroup of G_2 we must show that $g^{-1}ng \in H_1$ for $h \in H_1$ and $g \in G_1$ but $\phi(g^{-1}hg) = [\phi(g)]^{-1}\phi(h)\phi(g) \in H_2$
   Since H_2 is normal subgroup of G_2. Therefor $g^{-1}hg \in H_1$.

1.5 Kernel

Let $f : G \to H$ be a homomorphism the kernel of f is the set K of all the elements of G which are carried by f onto the neutral element of H.

$$K = \{X \in G : f(x) = e\}$$

Theorem 1.5.1 [7]Let $F : G \to H$ be homomorphism

i. The kernel of F is normal subgroup of G.

ii. The Range of F is a subgroup of H.

Proof:

Let K denote the kernel of F, if $a, b \in K$, this means that $F(a) = e$ and $F(b) = e$, thus $F(ab) = F(a)F(b) = ee = e$. Hence $ab \in K$.

If $a \in K$, then $F(a) = e$, thus $F(a^{-1}) = [F(a)]^{-1} = e^{-1} = e$, so $a^{-1} \in K$.

Finally, if $a - K$ and $x \in G$, then $F(xax^{-1}) = f(x)f(a)f(x^{-1})$ which shows that $XaX^{-1} \in K$. Thus, K is normal subgroup of G.

Now we must prove part (ii). If $f(a)$ and $f(b)$ are in the range of f, then their product $f(a)f(b) = f(ab)$ is also in the range of f

If $f(a)$ is in the range of F, it's inverse is $[f(a)]^{-1} = F(a)^{-1}$, which is also in the range of F. Thus, the range of F is a subgroup of H.

References

[1] Book 1.

[2] Book 2.

[3] Book 3.

[4] Book 4.

[5] Book 5.

[6] Book 5.

[7] Book 5.

[8] Book 5.

[9] Book 5.

[10] Book 5.